ПРОБЛЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОМУНИКАЦИИ. ФИШИНГ

Бондаренко А.С. ст.гр. РЭА-12д
Научный руководитель доц. Самойлова Ж.Г.
Восточноукраинский национальный университет им. В. Даля
Технологический институт

Целью работы является исследование защиты телекоммуникационных сетей от «фишинга».

В телекоммуникационной системе можно выделить три варианта воздействия на информацию:

- Задержка в передаче информации. Телекоммуникационная система может обеспечить абсолютно достоверную передачу информации, но время ее передачи может оказаться столь длительным, что она потеряет свою актуальность для потребителя.
- Искажение или нарушение целостности информации. При этом часть информации может быть утеряна, подменена другой информацией, либо к исходной информации может быть добавлена информация, искажающая исходную (например, вирусы).
- Несанкционированный доступ к информации, т.е. нарушение конфиденциальности информации[1].

Фишинг – (от англ. fishing рыбная ловля, выуживание) – вид интернет мошенничества с использованием социальной инженерии для получения доступа к конфиденциальной информации пользователей – логинам и паролям[2].

Одним из видов фишинга может быть массовая рассылка от имени какого либо банка или сервиса, с просьбой отправить в ответ ваши данные, т.к. это необходимо например для проверки безопасности или еще чего-либо (в основном такие запросы очень правдоподобны и доверчивые пользователи отправляют свои данные не задумываясь).

Другой вид фишинга это подделка сайта оригинала - фишеры регистрируют доменные имена, совпадающие с именами известных компаний, в которых часть латинских букв заменена на буквы национальных алфавитов, о чем мы будем говорить, рассматривая проблему внедрения кириллицы в доменной адресации. Однако еще до появления многоязычных доменов фишеры успешно обманывали пользователей, заменяя, например, символ «I» на цифру «1».

Средства Phishing-мошенничества с каждым днем продолжают расти не только количественно, но и качественно. В отчете за январь 2007 года по данным Anti-Phishing Working Group (www.anti-phishing.org) приводятся следующие цифры:

- Количество уникальных фишинговых атак - 29930
- Количество уникальных фишинговых сайтов - 27221
- Количество торговых марок, похищенных фишерами в январе - 135
- Страна, в которой в январе было открыто максимальное количество фишинговых сайтов - Соединенные Штаты Америки
- Количество сайтов, содержащих некоторую часть подлинного имени сайта в адресе - 24.5 %[4]

Способы доставки фишинговых сообщений можно разделить на следующие группы:

✓ *Электронная почта и спам.* Используя методы и инструментальные средства спамеров, фишеры могут разослать специальные сообщения на миллионы адресов электронной почты в течение нескольких часов (или минут, если задействовать распределенные бот-сети).

✓ *Фишинг-атаки с использованием web-контента.* Следующий метод фишинг-атак заключается в использовании вредоносного содержимого web-сайта. Этот контент может быть включен в сайт фишера, или сторонний сайт.

✓ *Фальсификация рекламных баннеров.* Реклама с помощью банера - очень простой метод фишинга. Он может использоваться для переадресации клиента на поддельный сайт организации.

✓ *IRC и передача IM-сообщений.* Так как эти каналы связи все больше нравятся домашним пользователям, и вместе с тем в данное программное обеспечение включено большое количество функциональных возможностей, число фишинг-атак с использованием этих технологий будет резко увеличиваться.

✓ *Использование троянских программ.* В данном случае, фишеры не только вытягивают из жертвы необходимую информацию, но и в дальнейшем используют ее компьютер для рассылки новых писем[3].

В результате проведенных нами исследований, можно говорить о том, что в данный момент существует только один метод защиты от фишинга - прекратить пересылку конфиденциальной информации через незащищенные каналы связи. Но на сегодня это выглядит нереальным. С развитием глобальных сетей и внедрением новых телекоммуникационных технологий решение проблем безопасности телекоммуникационных систем не может быть осуществлено потребителем услуг,

оператором связи или даже целой страной. Это под силу только всему мировому сообществу. Постоянно создаются новые средства и способы информационной безопасности, системы шифрования, защиты от вторжений, распознавания и т.д. Однако ситуация обостряется тем, что необходимо обеспечить баланс между основополагающими правами граждан и интересами общества, а в разных странах свое понимание этих прав и интересов. Определенный шаг по унификации требований был сделан в Будапеште в ноябре 2001 года, где была принята Конвенция о компьютерных преступлениях[5].

Используемые источники:

[1]. http://www.osp.ru/win2000/2008/02/4887833
[2]. http://www.microsoft.com/ru-ru/security/online-privacy/phishing-scams.aspx
[3]. http://it-web-log.ru/2012/02/fishingovaya-ataka
[4]. http://www.kaspersky.ru/internet-security-center/threats/spam-phishing
[5]. http://www.asterisk.by/node/819